

REMARKS¹

Claims 1, 3-38, and 40-81 remain pending in this application, with claims 1 and 38 being independent.

In the Request for Reconsideration filed with the Request for Continued Examination on January 4, 2008, Applicant responded to the Examiner's repeated rejections of the pending claims. However, the Examiner found Applicant's arguments not persuasive, and maintained the same rejections in the outstanding Office Action. Applicant respectfully traverses the following rejections which are all under 35 U.S.C. § 103(a):

I. rejection of claims 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 57, 58, 62, and 74-81 as unpatentable over Murphy et al. (U.S. Patent No. 6,226,744) in view of Ishibashi et al. (U.S. Patent Publication No. 2004/0006695);

II. rejection of claims 6, 9, 18, 22, 23, 43, 51, 55, 59, 60, and 66 as unpatentable over Murphy et al. in view of Ishibashi et al., and further in view of de Jong et al. (U.S. Patent No. 7,085,840);

III. rejection of claims 7, 8, 44, and 45 as unpatentable over Murphy et al. in view of Ishibashi et al. and de Jong et al., and in further view of Chang et al. (U.S. Patent No. 6,715,082) and Yu et al. (U.S. Patent No. 6,067,621);

IV. rejection of claims 19, 24, 26, 56, and 61 as unpatentable over Murphy et al. in view of Ishibashi et al., and further in view of Teicher et al. (U.S. Patent No. 6,257,486);

V. rejection of claims 25, 36, 37, 72, and 73 as unpatentable over Murphy et al. in view of Ishibashi et al., and further in view of Geer, Jr. et al. (U.S. Patent No. 6,192,131);

VI. rejection of claims 28-31, 34, 63-65, 67, and 68 as unpatentable over Murphy et al. in view of Ishibashi et al., de Jong et al.,

¹ The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

Chang et al., and Yu et al., and further in view of Baird, III et al. (U.S. Patent No. 6,732,278); and

VII. rejection of claims 32, 33, 35, and 69-71 as unpatentable over Murphy et al. in view of Ishibashi et al., de Jong et al., Chang et al., Yu et al., and Baird, III et al., and further in view of Teppler (U.S. Patent No. 6,792,536).

Regarding the rejection of claims 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 57, 58, 62, and 74-81 as unpatentable over Murphy et al. and Ishibashi et al., Applicant previously pointed out that, contrary to the Examiner's allegation, Murphy et al. at least fails to teach or suggest a PAD comprising "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key," as required by independent claim 1. See Request for Reconsideration of January 4, 2008, at 3-5. Ishibashi et al. fails to cure the deficiencies of Murphy et al. See Request for Reconsideration of November 5, 2007, at 5-7.

Recognizing that Murphy et al. does not teach or suggest a PAD comprising "at least one storage medium storing at least one CA public key," the Examiner points to Ishibashi et al., which teaches a memory device that may store a public key of a certificate authority. Office Action at 2-3. However, the Examiner failed to articulate a reason why it would be obvious to combine Ishibashi et al.'s memory device with Murphy et al.'s disclosure to result in the claimed PAD device. See M.P.E.P., § 2142, 8th Ed., Rev. 6 (Sept. 2007) ("The key to supporting any rejection under 35 U.S.C. § 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious."). As discussed in detail below, Murphy et al. actually teaches away from the above-quoted claim element, and therefore cannot be combined with Ishibashi et al.

Specifically, Murphy et al. teaches the following:

"[A] Certified Authority (CA) distributes smart card 10 to a user Smart card 10 stores user information provided by the CA, . . . or personal information provided by the user" Murphy et al., 5:54-60; and

"The user inserts smart card 10 into smart card reader 12 The user inserts smart card reader 12 into a 3.5 inch floppy disk drive for client terminal 14 Client computer 14 uses a web browser to access secure gateway server 18 via WWW 16 Secure gateway server 18 initiates authentication of the user of smart card 10 using authentication module 32. . . . Authentication module 32 then retrieves authentication information from database 26 In this embodiment of the invention, the authentication information was stored in database 26 by the same CA that issued smart card 10 to the user. An authentication profile is created for every user, with each authentication profile having authentication information that matches the user information stored on smart card 10." Murphy et al., 5:66 - 6:40, and Fig. 1.

Clearly, in Murphy et al., authentication is carried out over the network and in particular, by storing the same set of information on the smart card and also on a server, and comparing the information stored on the smart card and the information stored on the server to determine if they match. As an example, if a certificate issued by a CA is used for the purpose of authentication, the same certificate will be stored on the smart card and in the database on the network and will be used by authentication module 32. Such an authentication process does not require the use of the public key of the CA by authentication module 32 and, therefore, it is entirely unnecessary to store the public key of the CA on the smart card.

For similar reasons, the fallacy becomes clear in the Examiner's allegation that because the smart card stores certificates issued from a CA, the smart card necessarily contains the public key of the CA. Even though the smart card may store a certificate issued by a CA, Murphy et al. does not teach storing the public key of the CA on the smart card, and it is unnecessary to store the public key of the CA on the smart card.

Thus, Murphy et al. at least fails to teach or suggest a PAD that comprises "at least one storage medium storing at least one CA public key," as recited in claim 1. Murphy et al. actually teaches away from this element. As a result, one of ordinary skill in the art would not combine Ishibashi et al. with Murphy et al.

Murphy et al. also fails to teach or suggest a PAD that comprises "a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key," as recited in claim 1. Ishibashi et al. does not cure this deficiency either.

The Examiner quoted the following from Murphy et al.:

"It is worthy to note that the specific data being stored and retrieved from the smart card in this example of a smart card interface module is in the form [of] a user's social security number (SSN) for use in authenticating the user. It can be appreciated, however, that any type of data could be stored or retrieved from the smart card, such as tickets, certificates, public/private keys, and so forth." Murphy et al., 7:22-28.

The Examiner stated that this quote from Murphy et al. teaches that the smart card can be used to authenticate certificates. Office Action at 3. However, the quote above merely states that various types of information, including certificates, may be used to authenticate a user. One of ordinary skill in the art would understand that authentication of a certificate is not the same as authentication of a user.

As Applicant previously pointed out, Murphy et al. fails to teach or suggest authentication of a certificate and, therefore, fails to teach or suggest at least "a processing component for authenticating [] one or more received digital certificates

using the at least one stored CA public key.” Request for Reconsideration of November 5, 2007, at 5.

Ishibashi et al. fails to cure this deficiency. As Applicant previously discussed, Ishibashi et al. describes two verification processes: mutual authentication between an IC card and a registration authority and validation of a parent card. Neither process includes authentication of a digital certificate using a stored CA public key. Particularly, the mutual authentication process, which is described in paragraphs [0161]-[0164] and shown in Fig. 4, mutually authenticates the IC card and the registration authority, but does **not** authenticate one or more digital certificates. The validation of the parent card, which is described in paragraphs [0194]-[0205] and shown in Figs. 8 and 9, validates the public-key certificate stored on the parent card, but does not use “at least one CA public key” stored on any storage medium. Request for Reconsideration of November 5, 2007, at 5-7.

In summary, Murphy et al. fails to teach or suggest “at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key,” as required by independent claim 1. Ishibashi et al. fails to cure these deficiencies of Murphy et al. Even though the Examiner attempted to combine Ishibashi et al. with Murphy et al. for a teaching of a storage medium storing a public key of a CA, the Examiner failed to articulate any reason why such combination would be obvious. In fact, as Applicant pointed out above, Murphy et al. teaches away from the claimed element and, therefore, teaches away from the combination with Ishibashi et al. The

Examiner thus failed to establish a prima facie case of obviousness. Applicant therefore respectfully requests that the rejection of claim 1 be withdrawn.

Independent claim 38 recites, inter alia,

storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA);

. . .

authenticating the one or more received digital certificates using the at least one stored CA public key.

For reasons similar to those stated above regarding claim 1, a prima facie case of obviousness based on Murphy et al. nor Ishibashi et al. has not been established with regard to claim 38. The rejection of claim 38 should be withdrawn.

Claims 2-5, 10-13, 15-17, 20, 21, 27, 39-42, 46-50, 52-54, 57, 58, 62, and 74-81 respectively depend from claims 1 and 38 and therefore respectively incorporate all elements of claims 1 and 38. For the same reasons stated above with regard to claims 1 and 38, the rejection of claims 2-5, 10-13, 15-17, 20, 21, 27, 39-42, 46-50, 52-54, 57, 58, 62, and 74-81 is improper and should be withdrawn.

Each of the other claim rejections was based in part on the Murphy et al. and Ishibashi et al. references. Applicant incorporates the arguments above regarding Murphy et al. and also incorporates the arguments presented in the Request for Reconsideration of November 5, 2007, with regard to the additional references relied upon for the 35 U.S.C. § 103(a) rejections. For at least the reasons presented in that paper, the other applied references do not compensate for the deficiencies of Murphy et al. and Ishibashi et al. Therefore, Applicant respectfully requests that the Examiner reconsider and withdraw these rejections.


In view of the foregoing remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 30, 2008

By: 

Qingyu Yin
Reg. No. 61,329